

**What Is Claimed Is:**

1 1. A method for facilitating secure transmission of an email message  
2 to anonymous recipients without divulging the identities of the anonymous  
3 recipients, comprising:  
4 identifying recipients of the email message, wherein the recipients can  
5 include known recipients, who can be identified by examining the email message,  
6 and anonymous recipients, who cannot be identified by examining the email  
7 message;  
8 generating a session key for the email message;  
9 encrypting a body of the email message with the session key;  
10 creating a recipient block for the email message that contains an entry for  
11 each recipient of the email message;  
12 wherein each entry in the recipient block contains the session key  
13 encrypted with a public key associated with the recipient to form an encrypted  
14 session key, so that only a corresponding private key held by the recipient can be  
15 used to decrypt the encrypted session key;  
16 wherein each entry additionally contains an identifier for the associated  
17 public key, so that each recipient can determine whether the recipient possesses  
18 the corresponding private key that can decrypt the encrypted session key;  
19 wherein identifiers for public keys belonging to known recipients are  
20 statistically unique;  
21 wherein identifiers for public keys belonging to anonymous recipients are  
22 not statistically unique; and  
23 sending the email message to the recipients.

1           2.       The method of claim 1, wherein identifiers for public keys  
2 belonging to anonymous recipients provide only enough information to exclude a  
3 large percentage of all possible corresponding private keys from being able to  
4 decrypt the body of the email message.

1           3.       The method of claim 2, wherein an identifier for a public key is  
2 formed by creating a hash of the public key.

1           4.       The method of claim 3, wherein an identifier for a public key  
2 belonging to an anonymous recipient is additionally modified so the identifier is  
3 not statistically unique;  
4           whereby the identifier cannot be used to uniquely identify the anonymous  
5 recipient; and  
6           whereby a recipient can use the identifier to exclude a large percentage of  
7 all possible corresponding public keys held by the recipient from matching the  
8 identifier.

1           5.       The method of claim 1, further comprising, - encrypting the body  
2 of the email message, including a checksum into the body of the email message,  
3 so that a recipient can examine the checksum to verify that the correct private key  
4 was used in decrypting the email message.

1       ~~6.~~       A method for facilitating secure transmission of an email message  
2 to anonymous recipients without divulging the identities of the anonymous  
3 recipients, comprising:  
4           receiving the email message at a recipient, wherein the email message  
5 includes,

1 a message body that has been encrypted with a session key,  
2 a recipient block that contains an entry for each recipient of  
3 the email message,  
4 wherein each entry in the recipient block contains the  
5 session key encrypted with a public key associated with the  
6 recipient to form an encrypted session key,  
7 wherein each entry additionally contains an identifier for  
8 the associated public key,  
9 wherein identifiers for public keys belonging to known  
10 recipients are statistically unique, and  
11 wherein identifiers for public keys belonging to anonymous  
12 recipients are not statistically unique;  
13 attempting to match a candidate public key held by the recipient with key  
14 identifier in the recipient block;  
15 if the candidate public key matches a key identifier,  
16 decrypting the associated encrypted session key using an  
17 associated private key to restore the session key,  
18 decrypting the message body using the session key, and  
19 examining a checksum in the message body to verify that  
20 message body was correctly decrypted.

1 7. The method of claim 6, wherein identifiers for public keys  
2 belonging to anonymous recipients provide only enough information to exclude a  
3 large percentage of all possible corresponding private keys from being able to  
4 decrypt the message body of the email message.

002007-2627960

1           8.       The method of claim 7, wherein an identifier for a public key is  
2       formed by creating a hash of the public key.

1           9.       The method of claim 8, wherein an identifier for a public key  
2       belonging to an anonymous recipient is additionally modified so the identifier is  
3       not statistically unique;  
4               whereby the identifier cannot be used to uniquely identify the anonymous  
5       recipient; and  
6               whereby a recipient can use the identifier to exclude a large percentage of  
7       all possible public keys belonging to the recipient from matching the identifier.

1           10.      A computer-readable storage medium storing instructions that  
2       when executed by a computer cause the computer to perform a method for  
3       facilitating secure transmission of an email message to anonymous recipients  
4       without divulging the identities of the anonymous recipients, the method  
5       comprising:  
6               identifying recipients of the email message, wherein the recipients can  
7       include known recipients, who can be identified by examining the email message,  
8       and anonymous recipients, who cannot be identified by examining the email  
9       message;  
10              generating a session key for the email message;  
11              encrypting a body of the email message with the session key;  
12              creating a recipient block for the email message that contains an entry for  
13       each recipient of the email message;  
14              wherein each entry in the recipient block contains the session key  
15       encrypted with a public key associated with the recipient to form an encrypted

00677292.100200

16 session key, so that only a corresponding private key held by the recipient can be  
17 used to decrypt the encrypted session key;  
18 wherein each entry additionally contains an identifier for the public key, so  
19 that each recipient can determine whether the recipient possesses the  
20 corresponding private key that can decrypt the encrypted session key;  
21 wherein identifiers for public keys belonging to known recipients are  
22 statistically unique;  
23 wherein identifiers for public keys belonging to anonymous recipients are  
24 not statistically unique; and  
25 sending the email message to the recipients.

1 11. The computer-readable storage medium of claim 10, wherein  
2 identifiers for public keys belonging to anonymous recipients provide only enough  
3 information to exclude a large percentage of all possible corresponding private  
4 keys from being able to decrypt the body of the email message.

1 12. The computer-readable storage medium of claim 11, wherein an  
2 identifier for a public key is formed by creating a hash of the public key.

1 13. The computer-readable storage medium of claim 12, wherein an  
2 identifier for a public key belonging to an anonymous recipient is additionally  
3 modified so the identifier is not statistically unique;  
4 whereby the identifier cannot be used to uniquely identify the anonymous  
5 recipient; and  
6 whereby a recipient can use the identifier to exclude a large percentage of  
7 all possible public keys belonging to the recipient from matching the identifier.

00677292-100200

1           14.    The computer-readable storage medium of claim 10, wherein prior  
2   to encrypting the body of the email message, the method further comprises  
3   including a checksum into the body of the email message, so that a recipient can  
4   examine the checksum to verify that the correct private key was used in  
5   decrypting the email message.

1           15.    A computer-readable storage medium storing instructions that  
2   when executed by a computer cause the computer to perform a method for  
3   facilitating secure transmission of an email message to anonymous recipients  
4   without divulging the identities of the anonymous recipients, the method  
5   comprising:  
6           receiving the email message at a recipient, wherein the email message  
7   includes,  
8                   a message body that has been encrypted with a session key,  
9                   a recipient block that contains an entry for each recipient of  
10           the email message,  
11                   wherein each entry in the recipient block contains the  
12           session key encrypted with a public key associated with the  
13           recipient to form an encrypted session key,  
14                   wherein each entry additionally contains an identifier for  
15           the associated public key,  
16                   wherein identifiers for public keys belonging to known  
17           recipients are statistically unique, and  
18                   wherein identifiers for public keys belonging to anonymous  
19           recipients are not statistically unique;  
20           attempting to match a candidate public key held by the recipient with key  
21   identifier in the recipient block;

09677292.100200

1 if the candidate public key matches a key identifier,  
2 decrypting the associated encrypted session key using an  
3 associated private key to restore the session key,  
4 decrypting the message body using the session key, and  
5 examining a checksum in the message body to verify that  
6 message body was correctly decrypted.

1 16. The computer-readable storage medium of claim 15, wherein  
2 identifiers for public keys belonging to anonymous recipients provide only enough  
3 information to exclude a large percentage of all possible corresponding private  
4 keys from being able to decrypt the message body of the email message.

1 17. The computer-readable storage medium of claim 16, wherein an  
2 identifier for a public key is formed by creating a hash of the public key.

1 18. The computer-readable storage medium of claim 17, wherein an  
2 identifier for a public key belonging to an anonymous recipient is additionally  
3 modified so the identifier is not statistically unique;  
4 whereby the identifier cannot be used to uniquely identify the anonymous  
5 recipient; and  
6 whereby a recipient can use the identifier to exclude a large percentage of  
7 all possible public keys belonging to the recipient from matching the identifier.

1 19. An apparatus that facilitates secure transmission of an email  
2 message to anonymous recipients without divulging the identities of the  
3 anonymous recipients, comprising:

00677292.100200

4 an identifying mechanism that is configured to identify recipients of the  
5 email message, wherein the recipients can include known recipients, who can be  
6 identified by examining the email message, and anonymous recipients, who  
7 cannot be identified by examining the email message;  
8 a key generation mechanism that is configured to generate a session key  
9 for the email message;  
10 an encryption mechanism that is configured to encrypt a body of the email  
11 message with the session key;  
12 a recipient block creation mechanism that is configured to create a  
13 recipient block for the email message that contains an entry for each recipient of  
14 the email message;  
15 wherein each entry in the recipient block contains the session key  
16 encrypted with a public key associated with the recipient to form an encrypted  
17 session key, so that only a corresponding private key held by the recipient can be  
18 used to decrypt the encrypted session key;  
19 wherein each entry additionally contains an identifier for the associated  
20 public key, so that each recipient can determine whether the recipient possesses  
21 the corresponding private key that can decrypt the encrypted session key;  
22 wherein identifiers for public keys belonging to known recipients are  
23 statistically unique;  
24 wherein identifiers for public keys belonging to anonymous recipients are  
25 not statistically unique; and  
26 a sending mechanism that is configured to send the email message to the  
27 recipients.

1 20. The apparatus of claim 19, wherein identifiers for public keys  
2 belonging to anonymous recipients provide only enough information to exclude a



002007" 2624960

3 large percentage of all possible corresponding public keys from being able to  
4 decrypt the body of the email message.

1 21. The apparatus of claim 20, wherein an identifier for a public key is  
2 a hash of the public key.

1 22. The apparatus of claim 21, wherein the recipient block creation  
2 mechanism is additionally configured to modify an identifier for a public key  
3 belonging to an anonymous recipient so the identifier is not statistically unique;  
4 whereby the identifier cannot be used to uniquely identify the anonymous  
5 recipient; and  
6 whereby a recipient can use the identifier to exclude a large percentage of  
7 all possible public keys held by the recipient from matching the identifier.

1 23. The apparatus of claim 19, further comprising a checksum  
2 mechanism that, wherein prior to encrypting the body of the email message, the  
3 checksum mechanism is configured to include a checksum into the body of the  
4 email message, so that a recipient can examine the checksum to verify that the  
5 correct private key was used in decrypting the email message.

1 ~~24.~~ An apparatus that facilitates secure transmission of an email  
2 message to anonymous recipients without divulging the identities of the  
3 anonymous recipients, comprising:  
4 a receiving mechanism that is configured to receive the email message at a  
5 recipient, wherein the email message includes,  
6 a message body that has been encrypted with a session key,

1 a recipient block that contains an entry for each recipient of  
2 the email message,  
3 wherein each entry in the recipient block contains the  
4 session key encrypted with a public key associated with the  
5 recipient to form an encrypted session key,  
6 wherein each entry additionally contains an identifier for  
7 the associated public key,  
8 wherein identifiers for public keys belonging to known  
9 recipients are statistically unique, and  
10 wherein identifiers for public keys belonging to anonymous  
11 recipients are not statistically unique;  
12 a matching mechanism that is configured to attempt to match a candidate  
13 public key belonging to the recipient with key identifier in the recipient block;  
14 a decryption mechanism, wherein if the candidate public key matches a  
15 key identifier, the decryption mechanism is configured to,  
16 decrypt the associated encrypted session key using a  
17 corresponding private key to restore the session key,  
18 decrypt the message body using the session key, and to  
19 examine a checksum in the message body to verify that  
20 message body was correctly decrypted.

1 25. The apparatus of claim 24, wherein identifiers for public keys  
2 belonging to anonymous recipients provide only enough information to exclude a  
3 large percentage of all possible corresponding private keys from being able to  
4 decrypt the message body of the email message.

